REMARKS/ARGUMENTS

1. Summary of the Office Action

Claim 4 stands rejected under § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-4 stand rejected under § 103(a) as allegedly being anticipated by U.S. patent no. 6,073,122 (hereinafter "Wool") in view of U.S. patent no. 5,392,353 (hereinafter "Morales").

Claims 5 stands rejected under § 103(a) as allegedly being anticipated by Wool and Morales, and further in view of Wood, D.; The DVB Project: Philosophy and Core System (hereinafter "Morales").

2. Response to § 112 Rejection

Claim 1 and Claim 4 have been amended so that the objection will be obviated.

Claim 1 has been amended by further specifying that data packets with an individual address are provided to the head-end. This amendment is based on the description, page 3, line 19. Furthermore, it is specified that data packets are inserted into transport packets of a digital transport stream at the head-end. This amendment is based on page 3, line 30. It is also clarified that the transport packets containing the data packets are subsequently scrambled. This amendment is based on the description, page 4, line 4. Thus, the subject-matter of amended claim 1 is to be found in the contents of the application as filed.

3. Response to § 103 Rejections

Applicant respectfully traverses this rejection for the reasons set out below, and ask the Examiner for reconsideration.

US 6 073 122 discloses a network environment for transferring encrypted multimedia information from a service provider using a transmitter, such as a head-end server, to one or more customers having set-top terminals (column 3, lines 49-53). The set-top terminal preferably executes a decode process to decrypt programs that a customer is entitled to, by using a corresponding stored package key, Sj, to decrypt a transmitted program key, Kp, and then using the program key, Kp, to decrypt the program (column 6, lines 41-45). As used therein, a package is a predefined set of programs, and a program can belong to one or more packages. A program is any continuous multimedia transmission of a particular length (column 4, lines 5-9). The head-end server preferably includes a processor and related memory, such as a data storage device (column 4, lines 44-46). The data storage device preferably includes a program database and a package database (column 4, lines 62-63). The program database preferably stores information on each program which will be transmitted by the head-end server (column 4, lines 63-66). The package database preferably stores information on each package offered by the head-end server to customers, including the name of each package and the corresponding package key, Sj. In addition to transmitting the encrypted program, the head-end server preferably transmits header information to the customers, containing a package pair for each package to which the program belongs. A package pair preferably includes an identifier of the package, as well as the program key Kp, encrypted by the corresponding package key, Sj. If a customer is entitled to a particular program, the set-top terminal will be able to decrypt the encrypted program key Kp, using the appropriate stored package key, SJ, and thereafter use the program key to decrypt the encrypted program (column 2, line 63-column 3, line 6). The package keys, SJ, can be downloaded from the head-end server to the set-top terminal using any suitably secure unidirectional or bi-directional protocol (column 4, lines 8-12).

Thus, US 6 073 122 fails to disclose sending a message to each receiver to which data needs to be transferred, including a key unique to the respective receiver. Instead, receivers can download package keys, which are unique to a pre-defined set of programs. US 6 073 122 further fails to disclose providing a table of unique keys with corresponding addresses of the respective

receivers at the head-end. Instead a package database stores information on each package offered by the head-end server to customers (column 5, lines 1-3). Other than the passage in column 4, lines 8-12, no information is given on the exact way in which each receiver receives the appropriate package keys. Thus, there is no information at the head-end linking keys to subscribers, let alone a table of keys unique to each respective receiver with corresponding addresses of the respective receivers. Also, US 6 073 122 fails to disclose providing data packets with an individual address of the respective receivers at the head-end (the publication is directed to broadcasting programs (column 3, lines 58-63)). Furthermore, US 6 073 122 does not teach inserting the data packets into transport packets of a digital transport stream at the head-end (column 3, lines 58-63 leaves the choice of transmission protocol open). Consequently, no disclosure is made of scrambling transport packets containing the data packets using the selected key (only the program key Kp is scrambled using SJ, and this scrambled key is then inserted into a header, i.e. not a subsequently scrambled transport packet). As more than one receiver can have a particular package key, SJ, US 6 073 122 naturally doesn't disclose descrambling the scrambled transport stream only at the receiver having the unique key used to scramble the scrambled transport packets.

US 5 392 353, when read together with US 4 591 906 and US 5 101 267, relates to ensuring privacy of communications point-to-point in a network with broadcast communications. US 5 392 353 discloses a method wherein secret messages are received and sent over a satellite system. A control center intercepts and process communications between all network stations. Each station is provided with signal selection, encrypting and decrypting equipment for isolating coded messages restricted to private use of that station. An auxiliary wireless transmission channel is used for conveying messages supplemental to programmed channels (column 3, lines 22-30). The system incorporates the features of US 4 591 906. The latter mentioned publication specifies that response units permit television viewers to communicate with a television station (column 5, lines 9-10 of US 4 591 906). These units have a channel selector to select channels which the television viewer wishes to see. A question channel is tuned by the channel selector. A T.V. station sends a modified radio frequency TV signal that is received by plural T.V. sets (column 6, lines 28-30 of US 4 591 906). At the T.V. station audio and video signals are generated. The video signal is modified by a T.V. ask system by encoding control and data bits

according to instructions given by a personal computer. These bits are inserted into even and odd fields of a frame of 525 lines (column 6, lines 49-50 of US 4 591 906).

US 5 392 353 does not itself provide information on the way the secret messages are communicated from the control center 3 to the subscriber stations 4.

In particular, US 5 392 353 does not disclose transferring data by means of a *digital* broadcast signal. The known method does not include sending a message to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver. Rather, in the method of US 5 392 353, the user of the receiver keys in the PIK by means of a separate telephone connection with a voice-response system, i.e. provides the key to the head-end, via a totally separate communications channel. Furthermore, there are no data packets with an individual address of at least one of said receivers and thus no data packets inserted into transport packets.

Summarizing the above, neither US 5 392 353 nor US 6 073 122 discloses a method including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver. Also, neither of the two publications discloses inserting data packets with an individual address into transport packets of a digital transport stream at the head-end, or scrambling said transport packets containing the data packets using the selected key.

By the interaction of these features with the other features, a method is provided enabling efficient and secure private data transfer in a broadcast environment. Each receiver can receive the digital transport stream, but the transport packets intended for one receiver can only be decrypted by the receiver having the corresponding unique key. Thus, the decryption key may be used as a mechanism for receivers to de-multiplex the transport stream to obtain the data packets intended for them. This allows the proportion of transport packets containing data intended for one particular receiver to be varied relative to the total number of transport packets transferred in a given time interval. The transmission is thus made more efficient. This effect is not mentioned

in the prior art, nor inherently provided by the prior art systems, so that the invention as defined in amended claim 1 provides a non-obvious contribution to the technical field.

Claims 2-5 relate to methods comprising all the features of amended claim 1. For this reason, it is submitted that their subject-matters are likewise patentable.

Claim 6 has been included on the basis of the description as filed, in particular page 4, lines 7-10, and page 3, line 13. Thus, it is submitted that no new subject matter has been added by this amendment.

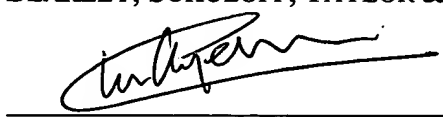
As claim 6 relates to a method comprising all the features defined in claim 1, it is submitted that the subject matter of claim 6 is also novel and non-obvious.

4. Conclusion

Having tendered the above remarks and amended the claims as indicated herein, Applicant respectfully submits that all rejections have been addressed and that the claims are now in a condition for allowance, which is earnestly solicited.

If there are any additional charges, please charge Deposit Account No. 02-2666. If a telephone interview would in any way expedite the prosecution of the present application, the Examiner is invited to contact Jaina Chua at (408) 947-8200 ext. 204.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP



Dated: March 1, 2004

Chze Koon Chua
Reg. No. 53,831

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200

WO 2585-dV

MK-Up

TITLE OF THE INVENTION

Method for transferring data from a head-end to a number of receivers

BACKGROUND OF THE INVENTION

The present invention relates to a method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream.

The use of a digital broadcast signal, such as a DVB signal, for transferring data to one or more receivers shows the advantage that available receivers with descramblers can be used to transfer the data from a head-end to the receiver. However, such a method would normally not allow for a data transfer in a secure and private manner as the data is accessible to all receivers listening to the digital transport stream.

US-A-5 392 353 relates to an interactive satellite broadcast network, wherein encrypted communications ensure privacy of communications point-to-paint in a network of interactive video stations interconnected by a broadcast network. Although a broadcast network is mentioned, this document refers to-point-point communications. Personal identification keys are used known only by the individual participating stations and a secure single central switching control center. The network control center intercepts communications encrypted as a function of the senders personal identification key and relays incoming communications designating the receiver in encrypted format as a function of the receivers personal identification key.

US-A-5 432 850 relates to a method and apparatus for secure data transmission, wherein a plurality of data frames are transmitted, each containing at least an encrypted data sequence employing the destination address as at least part of a decryption key. At the receiver side,

the encrypted data sequence is decrypted by employing the local address of the 20 receiver as at least part of the decryption key. In this known system each station can operate as a transmitting station using both the destination address and source address to encrypt the data.

EP-A-O 808 048 relates to a multimedia information service access, wherein a client can establish a connection with a server where desired multimedia information is resident. By selecting the desired multimedia information and providing a client information identifying this location of the user, the multimedia information is delivered by the server to a bridging apparatus through a switched network. It is indicated that the delivery of the multimedia information can be secured by comparing the client information to a segmented list to determine whether the client is authorized to receive the requested multimedia information.

The article "Internet Armor" by w. Stallings, Byte, vol. 21, no. 12, December *1996*, page 127-134, describes a method to provide secure IP package by encrypting the IP 'packet and providing a new IP header with the destination address. This document however relates to transfer data through the Internet.

BRIEF SUMMARY OF THE INVENTION

The present invention ~~aims to~~ provides a method of the above-mentioned type wherein privacy and security of the data transfer can be provided to each receiver.

According to the invention a method of the above-mentioned type is provided, including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver, loading the unique key in the descrambler of the respective receiver, providing a table of unique keys with corresponding addresses of the respective receivers at the head-end, providing data packets with an individual address of at least one of said receivers, inserting said data packets into transport packets of a digital transport stream, selecting a key from said table in accordance with the address of the data packets, scrambling said transport packets using the selected key, broadcasting the digital transport stream, receiving the digital transport stream at one or more receivers and descrambling the scrambled

transport packets of the digital transport stream only at the receiver having the unique key used to scramble the scrambled transport packets.

In this manner a method is obtained wherein each receiver attempting to descramble the broadcast signal will fail to descramble the signal except ~~accept~~ for the receiver(s) having the unique key(s) used to scramble the transport packets in which the data packets are inserted which are intended to be received by this receiver. This results in the desired privacy and security for the data transfer between the head-end and the receiver.

In a preferred embodiment for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being scrambled with a unique key corresponding with the individual address of the corresponding data packets.

In this manner data transfer with privacy and security is provided for a number of receivers requesting the transfer of data.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The invention will be further explained by reference to the drawings in which an embodiment of the invention is schematically shown.

DETAILED DESCRIPTION OF THE INVENTION

In this preferred embodiment the method is used to transfer data requested by a receiver from the Internet to the receiver on a digital broadcast signal or digital transport stream, so that an Internet connection is obtained with a high speed transfer of data to the receiver according to

the Internet Protocol. However the method described can also be used to transfer data to receivers at their request or initiated by the head-end in another manner.

In the drawing a DVB system is very schematically shown by way of example, the system comprising head-end equipment 1 which will be indicated hereinafter by head-end, and a large number of subscribers having a receiver 2, only one of which is shown in the drawing. The receiver 2 includes a descrambler 3 co-operating with a smart card 4 in a usual manner. The descrambler 3 is used to descramble DVB services requiring a subscription. The receiver 2 is connected to the Internet 5 in a manner not further shown, for example by a well-known modem. If the receiver 2 requests the download of data, the data will be transferred to the receiver 2 via the head-end 1 by means of a broadcast signal in the following manner.

According to the internet protocol the data includes an IP or MAC address of the receiver 2 requesting the data to be transferred to this receiver. Each receiver 2 for which the head-end 1 receives data packets with an individual address, i.e. the IP or MAC address, is sent a so-called Entitlement Control Message or ECM with a control word or key which is unique to the receiver 2. This message is encrypted using an individual key which is stored in the smart card 4. At the head-end 1 the unique keys with the corresponding individual addresses are stored in a table 6. At the receiver(s) 2 to which an ECM is sent, the smart card 4 decrypts the received message using its individual key to obtain the unique key. The decrypted key is loaded into the descrambler 3 for future use.

At the head-end 1, the data packets for a specific receiver 2 requesting the transfer of data, are inserted into transport packets of the digital transport stream. Generally, the data packets are larger than the transport stream packets, so that the data packets are split and thereafter inserted into a number of transport stream packets. Before scrambling the transport stream packets containing the data packets, the head-end checks the IP or MAC address and selects the corresponding unique key from the table 6, which key is used to scramble the transport stream packets.

Each receiver 2 to which ~~listening to~~ the digital broadcast signal is transferred attempts to descramble the transport stream packets of the digital transport stream, wherein however only at the receiver 2 having the unique key used for scrambling the transport stream packets, the descrambling process will be successful. In this manner only one receiver 2 will descramble the scrambled transport stream packets to thereby obtain the IP data packets.

From the above it will be clear that the described method results in a transfer of data with privacy and security for each receiver 2 requesting a data transfer. Moreover, this transfer with privacy and security is achieved while using existing DVB or MPEG scrambling and descrambling equipment.

Generally, a number of receivers 2 will request the transfer of data. This is no problem as the head-end 1 will provide a table 6 including key/address combinations for each receiver 2 requesting a data transfer. The capacity of a digital broadcast signal is sufficient to transfer IP data packets to a large number of receivers 2. As the IP data packets for each particular receiver will be inserted into a number of transport packets wherein only these transport packets are scrambled using the unique key for this particular receiver, data transfer will still take place in a private and secure manner.

The data packets can be inserted into transport stream packets of a digital transport stream which is used for the transfer of data only. As an alternative the data packets can be inserted into transport stream packets of a DVB transport stream as the capacity of such a transport stream is far more than necessary for transferring the video information.

Although in the preferred embodiment the method is used to transfer IP data packets, the described method can ~~5~~ also be used to transfer data from other sources than the Internet. Further, it is noted that instead of an ECM another type of message may be used to transfer a unique key to a receiver.

Annotated Marked-up Drawings

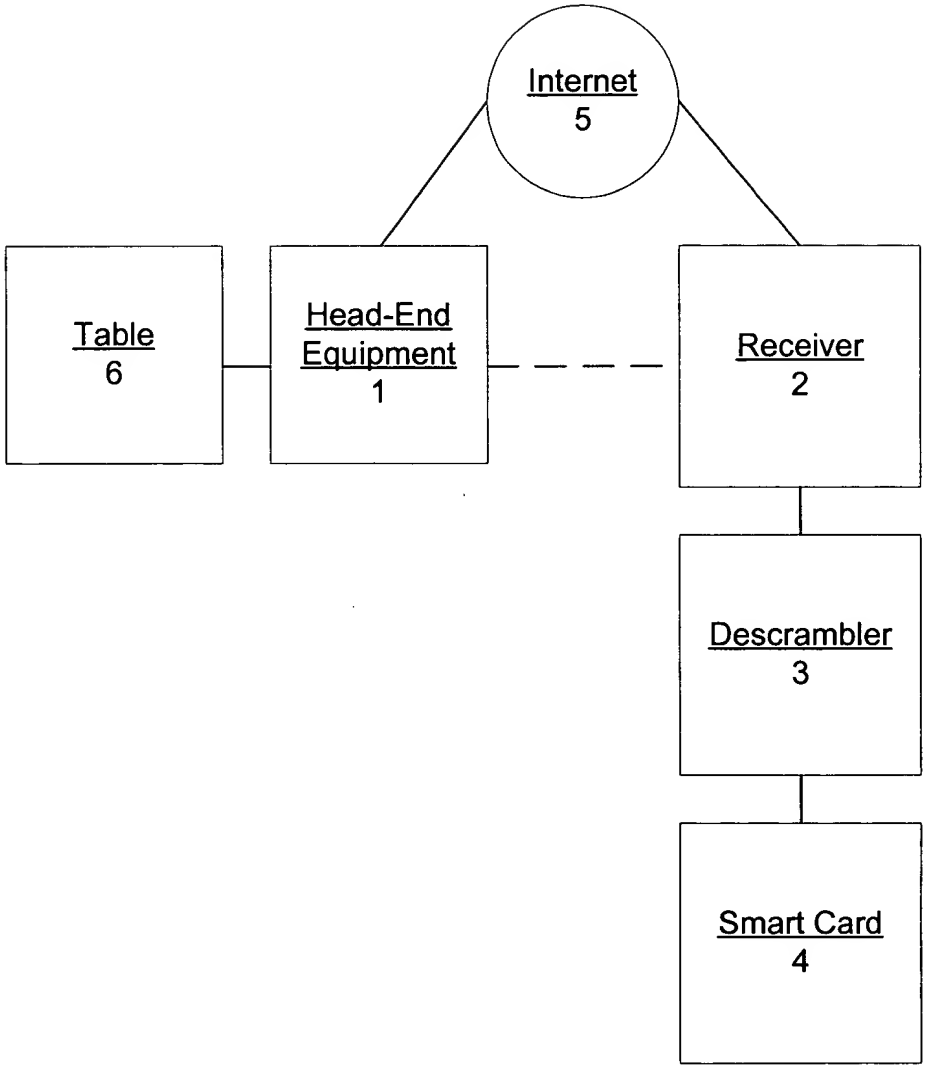


Figure 1